

# **EXHIBIT 13**

**From:** Cline, Brad [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=C1DA7AFA0BCE413F9C32CE66040660F3-CLINE, BRAD]  
**Sent:** 3/16/2018 11:50:59 PM  
**To:** Johnson, Rani [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0ee57945f15e47b3abaa99a59170ad3f-Johnson, Ra]  
**Subject:** Updated slides  
**Attachments:** 032018DOITMajorProjectPortfolio\_Draft.pptx

Hi Rani,

Here are the updated slides. Let me know if you want any other changes.

2 - Jazz Hands.

8 - I closed out the Gsuite portion, the original scope is complete and updated the 365 portion, if you concur that project is back on track.

9

17

20 - No changes, on track.

22 - Exchange and SQL complete, we also completed internal DNS and DHCP, Skype is the last on this project.

29 - Was sidelined for the 365 project, back on track.

33

34

35

39

Second 39 ?

40

44

# MAJOR PROJECT PORTFOLIO

MARCH 2018

DEVELOPMENT, OPERATIONS & INFORMATION TECHNOLOGY (DOIT)

DOIT Lead – Eric Quitugua  
 Business – Enterprise  
 Executive Sponsor – Joe Kim, Rani Johnson, Tim Brown



## #6 – ENTERPRISE ACCESS MANAGEMENT (STANDARDS & AUDIT)

<p><b>Description</b>            Access management describes the management of individual identities, their authentication, authorization, roles, and privileges within the enterprise in order to minimize security risks associated the use of privileged and non-privileged access.</p> <p><b>Scope:</b></p>	<p><b>KPIs</b></p> <p><b>Timeline</b></p>																																																											
<p><b>Budget</b></p> <table border="1"> <thead> <tr> <th>Q1 18</th><th>Q2 18</th><th>Q3 18</th><th>Q4 18</th><th>TOTAL</th></tr> </thead> <tbody> <tr> <td>\$0</td><td>\$0</td><td>\$0</td><td>\$0</td><td>\$0</td></tr> </tbody> </table> <p><b>Issues, Risks &amp; Dependencies</b></p> <table border="1"> <thead> <tr> <th>Cat No.</th><th>Description</th><th>Action Required</th></tr> </thead> <tbody> <tr> <td>I.1</td><td>Concept of least privilege not followed as a best practice</td><td>ID existing permission levels within the enterprise Work with teams to decommission use of shared accounts</td></tr> <tr> <td>I.2</td><td>Use of shared accounts throughout internal and external applications</td><td></td></tr> </tbody> </table>	Q1 18	Q2 18	Q3 18	Q4 18	TOTAL	\$0	\$0	\$0	\$0	\$0	Cat No.	Description	Action Required	I.1	Concept of least privilege not followed as a best practice	ID existing permission levels within the enterprise Work with teams to decommission use of shared accounts	I.2	Use of shared accounts throughout internal and external applications		<p><b>Key Milestones / Status</b></p> <table border="1"> <thead> <tr> <th>Ph.</th><th>Milestone</th><th>Start</th><th>Finish</th><th>Status</th></tr> </thead> <tbody> <tr> <td>1</td><td>Conduct risk audit and risk assessment against privileged and non-privileged user accounts</td><td>10/1/2017</td><td>11/30/2017</td><td>Complete</td></tr> <tr> <td>2</td><td>Prioritize risk against security standards and guidelines</td><td>12/1/2017</td><td>12/31/2017</td><td>In Progress</td></tr> <tr> <td>3</td><td>Identify high risk accounts for remediation</td><td>12/1/2017</td><td>12/31/2017</td><td>In Progress</td></tr> <tr> <td>4</td><td>Validate privilege levels and access permissions</td><td>1/1/2018</td><td>2/28/2018</td><td>In Progress</td></tr> <tr> <td>5</td><td>Align access controls and permissions to security standards and guidelines</td><td>1/1/2018</td><td>2/28/2018</td><td>In Progress</td></tr> <tr> <td>6</td><td>Track remediation and map to access control guidelines and standards</td><td>Q1 2018</td><td>Q1 2018</td><td>Not Started</td></tr> <tr> <td>7</td><td>Document results and establish repeatable security assessment methodology for continuous monitoring</td><td>Q1 2018</td><td>Q1 2018</td><td>Not Started</td></tr> </tbody> </table>	Ph.	Milestone	Start	Finish	Status	1	Conduct risk audit and risk assessment against privileged and non-privileged user accounts	10/1/2017	11/30/2017	Complete	2	Prioritize risk against security standards and guidelines	12/1/2017	12/31/2017	In Progress	3	Identify high risk accounts for remediation	12/1/2017	12/31/2017	In Progress	4	Validate privilege levels and access permissions	1/1/2018	2/28/2018	In Progress	5	Align access controls and permissions to security standards and guidelines	1/1/2018	2/28/2018	In Progress	6	Track remediation and map to access control guidelines and standards	Q1 2018	Q1 2018	Not Started	7	Document results and establish repeatable security assessment methodology for continuous monitoring	Q1 2018	Q1 2018	Not Started
Q1 18	Q2 18	Q3 18	Q4 18	TOTAL																																																								
\$0	\$0	\$0	\$0	\$0																																																								
Cat No.	Description	Action Required																																																										
I.1	Concept of least privilege not followed as a best practice	ID existing permission levels within the enterprise Work with teams to decommission use of shared accounts																																																										
I.2	Use of shared accounts throughout internal and external applications																																																											
Ph.	Milestone	Start	Finish	Status																																																								
1	Conduct risk audit and risk assessment against privileged and non-privileged user accounts	10/1/2017	11/30/2017	Complete																																																								
2	Prioritize risk against security standards and guidelines	12/1/2017	12/31/2017	In Progress																																																								
3	Identify high risk accounts for remediation	12/1/2017	12/31/2017	In Progress																																																								
4	Validate privilege levels and access permissions	1/1/2018	2/28/2018	In Progress																																																								
5	Align access controls and permissions to security standards and guidelines	1/1/2018	2/28/2018	In Progress																																																								
6	Track remediation and map to access control guidelines and standards	Q1 2018	Q1 2018	Not Started																																																								
7	Document results and establish repeatable security assessment methodology for continuous monitoring	Q1 2018	Q1 2018	Not Started																																																								

10/16/2017 Update – Identity management continues to be a concern. Appropriate checks are in place to grant access but audit of access is not consistently implemented. Multi-Factor authentication should also be utilized in more environments. A risk assessment will be completed by 12/31

Review Roles

Review Membership

Implement MFA for high value areas

VPN

Determine volume through GlobalProtect